SECTIGO

A WHITE PAPER FROM SECTIGO

Digital Identities for Identity and Access Management

Secure Digital Identity for the Enterprise

One of the leading attacks on an Enterprise occurs when the attacker impersonates a legitimate user or device to steal intellectual property, or otherwise harm the business operations. A strong digital identity is the best proven method to prevent a digital impersonator.

Sectigo offers a strong digital identity using Public Key Infrastructure (PKI) technology. This is the same technology used by governments and financial institutions. The Sectigo digital identity is made up of two components:

1. A private cryptographic key that is never shared in the authentication process.

In a password based system, the user/device sends the password to the service being accessed, where the service then compares the password to the value previously stored. The attacks involve tricking the user to enter their password into a fraudulent replica of the website, stealing the password in transit, stealing it from the service that has the password stored or in a brute force attack by trying every possible password.

In the PKI method, the service accessed sends a challenge to the private key, which in turn, signs the challenge and returns it to the service as "proof of possession" of the private key. Unlike the password approach, there is no risk of the private key being stolen during authentication as the private key never leaves the client. As well, the length of the private key would require decades to brute force attack, even with the world's fastest computers versus hours for an eight-character password. Users find managing multiple, password difficult, resulting in the selection of weak passwords or reusing passwords across multiple systems. Hackers can easily compromise these passwords through social engineering and other duplicitous methods.

The private key is often placed into a software or hardware container that only allows the private key to perform a cryptographic operation after a PIN or biometric check to ensure the owner is operating the private key.

2. A digital certificate.

The certificate contains a public key that is paired with the secret private key. The public key is the only one capable of deciphering, verifying the signature. The certificate also includes the unique name of the authorized owner of the private key. The public key and unique name are cryptographically bound together by a Certification Authority (CA). Any attempt to tamper with either the public key or unique identity is detected.

Unlike other vendors, Sectigo offers both **Elliptic Curve** and **RSA** keys. The Elliptic Curve key is newer technology that offers much faster cryptographic operations, improving the user experience and decreasing the load on your servers. At the same time, its strength is better than that of the RSA for the same key length. This is most noticeable on constrained devices such as mobile, tablet, IoT device, or heavily-loaded servers.

The Sectigo digital identity provides the Enterprise three layers of protection: **Authentication**, **Encryption** and a **Digital Signature**. Security should not reduce the productivity of the Enterprise; it boosts productivity by reducing password resets, enables online forms, and by providing services not otherwise available in a less-secure implementation.

> The Sectigo digital identity provides the Enterprise three layers of protection: Authentication, Encryption and a Digital Signature.

- **Authentication:** As previously described, PKI provides strong authentication. In the following Enterprise use cases, an additional level of security is available in the form of a PIN. Since the PIN never leaves the client, there is no need to change it frequently as you would have to with a password.
- **Encryption:** In the unlikely case that an attacker circumvents the authentication, or for privacy, the same digital identity can be used to encrypt the information. This ensures that only authorized key holders can view the confidential information. The encryption private key may be placed into an escrow provided by Sectigo, so that it can be recovered by the owner in the event their copy is no longer available, to decrypt existing files.

- **Digital Signature:** The same digital identity can cryptographically sign documents, application code or commands. Any attempt to tamper with the document, code or command would be mathematically detected by the recipients. For example, a contract with a partner. Since a copy of the digital identity used for encryption is often held in escrow, the Enterprise would create a second digital identity used only for digital signature that has no other copy. Doing so confirms that the document (or other entities signed) came from the signator and no one else. This approach of using a 2nd key not backed up or shared with anyone else is called non-repudiation.

Enterprise Use Cases

The Sectigo digital identity can be used in several Enterprise applications, fully supported by automated life cycle management of the digital identity. A digital identity prevents malware from stealing user identity and/or unencrypted intellectual property, while improving the effectiveness of your business and employees.

- **Browser and Web Server through SSL:** Sectigo offers three types of certificates trusted by the world-wide web browsers: Domain Validated, Organization Validated and Extended Validation. The validation level indicates how rigorously the owner of the certificate is vetted.
  For servers within an Enterprise, certificates can be issued from a private CA where the customer has total control of the certificate contents and issuance process while still being trusted from browsers within the Enterprise.

Digital identity prevents malware from stealing user identity and/or unencrypted intellectual property, while improving the effectiveness of your business and employees.

- **Virtual Private Networks (VPN) Authentication:** By issuing a digital identity to the employee's device, authentication no longer requires plastic tokens or mobile apps. Authentication can be totally invisible or complemented by a PIN, saving valuable employee time by eliminating the need to remember passwords, and time wasted looking for plastic tokens, or mobile applications.
- **Network Devices Authentication:** Place a digital identity into a Windows desktop, server, networking equipment or WiFi access points. Only authorized devices can connect to your corporate network, eliminating the risk of malware being inadvertently installed in the network, or the loss of intellectual property to unauthorized devices.
- **Internet of Things (IoT) Security:** A digital identity installed on your IoT device, a user's device or application ensures that only trusted IoT devices can connect to your network. The IoT device will only accept instructions from or send data to authorized applications and users who also possess a digital identity. The digital certificate may also be used to establish a TLS session with other IoT devices or servers.
- **Secure Email through S/MIME Protocol:** A digital identity installed in Windows Outlook or your mobile device's mail application ensures all intellectual property is encrypted during transmission and when stored on your mail server. Should an attacker manage to gain access to your mail server, by-passing authentication and firewalls, the attacker won't be able to read your encrypted emails. In addition, when a publicly-trusted digital identity is used, recipients can verify that the sender is truly the person that sent the email and not an attacker posed to steal credentials or intellectual property. The Trusted Advisors at Sectigo will propose solutions with third-party products for a 100% encryption solution that is invisible to your employees and partners, while allowing the Enterprise to scan email entering or leaving the Enterprise.
- **Mac/Windows Login:** Avoid long, difficult to remember passwords that change every 90 days by replacing your login with a a digital identity. These digital identities are stored on a third-party smart card or USB token for portability across employee-accessible devices. The smart card, like your chip-based credit card, can be contact or contact-less. Microsoft Hello for Business biometric or PIN is used with certificate authentication, but does not require smart card. The certificate may be stored in the Trusted Platform Module (TPM) chip for hardware-level security. TPM chips are now built into all Windows 10 machines.

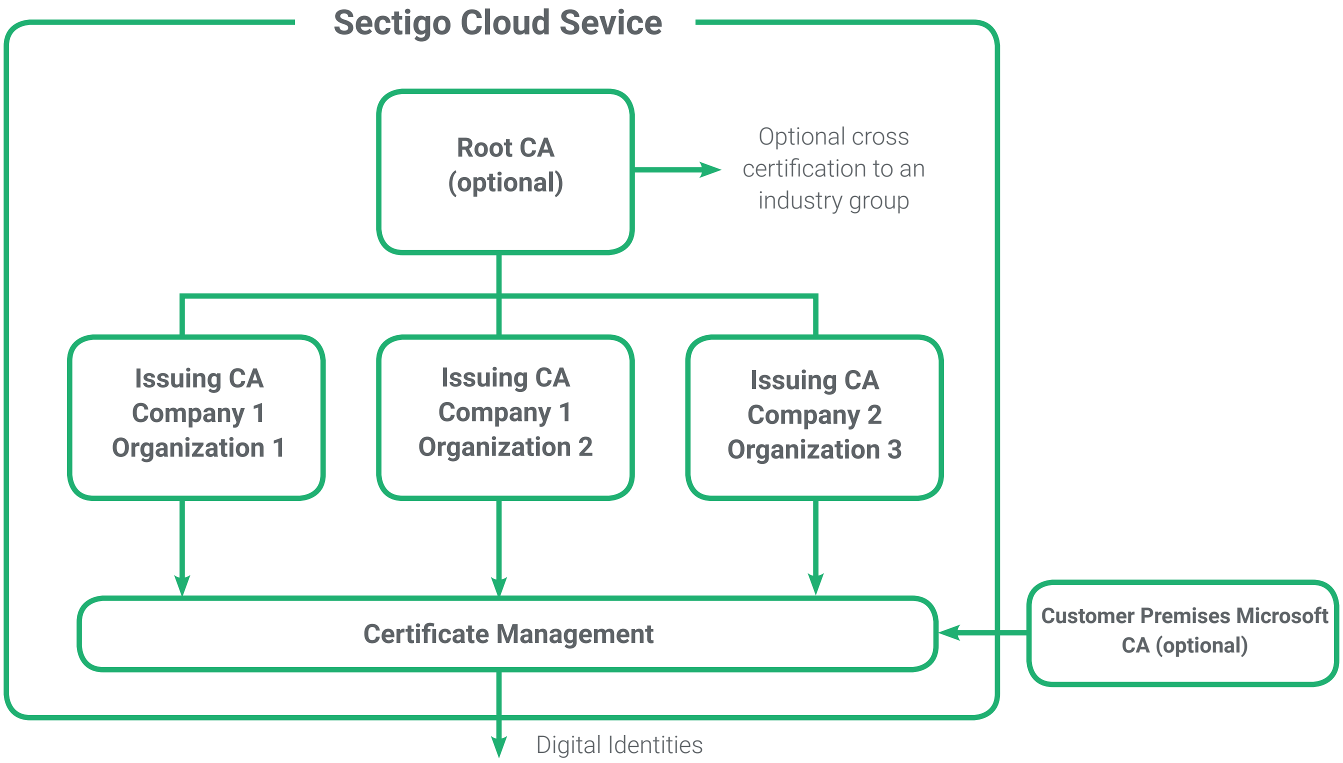
- **Single sign-on to Cloud Applications:** Today's Enterprise employees have access to a wide variety of cloud services, in some cases, using an Identity as a Service or Federation product. Substituting a digital identity from Sectigo instead of a password ensures invisible yet secure access to cloud services without the need to remember multiple user names and passwords.
- **Single sign-on to the Enterprise Web Portal:** The Enterprise often uses a Web Single-Sign product to provide access to all their resources in the corporate portal. By adding a Sectigo digital identity, the Enterprise can turn on a browser's built-in client side SSL to ensure access is only granted to authorized employees, partners or customers in an invisible and secure manner.
- **Mobile Device access to the Enterprise WiFi:** Employees using tablets and mobile devices need ready access to the corporate wireless network, while at the same time preventing unauthorized access to corporate resources. By installing a digital identity, only authorized devices can connect to the network. The use of a digital identity eliminates the need to change the password in conjunction with MS Windows password rules, or unauthorized access as there is no password to share. Employees always have access to the network in a transparent manner with no need for the IT Administrator to update a MAC address on the WiFi base station as employees change devices while blocking an unauthorized user in possession of a shared password.
- **File Encryption:** Using a Digital ID, employees can encrypt the files on their desktop, company servers or cloud servers for authorized individuals or themselves. This prevents unauthorized viewing of the content from a rogue server administrator, or attackers who have defeated the authentication controls.
- **Enterprise Mobility Management:** The applications provided by EMM vendors, such as Email and Browser, use digital identities for authentication, encryption and digital signatures. The third party EMM products integrate with Sectigo to provide the digital identities. For email applications, the same digital identity is provided to the mobile and Outlook mail application so that emails can be decrypted for an employee using both devices. The certificates are stored in a directory, so that sender's can encrypt for a recipient.
- **Code Signing:** Ensure your custom enterprise application is code-signed for trusted installation on the device.

- **Microsoft Virtual Smart Card (MVSC):** Starting with Windows 10 in July 2016, Microsoft mandated that all machines running the Microsoft operating system must possess a Trusted Platform Module (TPM). Prior to this, only high-end machines possessed a TPM. The TPM is a smart card chip built into the electronics of your computer. The TPM hardware protects the private key from being copied from your machine, ensuring that an attacker cannot impersonate the owner. The stronger key protection is used by all the PKI use cases on the Windows machine. With this improved key protection, it's no longer necessary to use a digital identity on a USB or card. The PKI approach is much simpler to use than a mobile or plastic second factor authenticator.
- **Microsoft Hello for Business:** This new capability is built on the same PKI technology used by the Microsoft Virtual Smart Card. Rather than the MVSC requiring a numerical PIN before performing the authentication function, the MVSC requires a biometric match of a facial image, fingerprint or voice.

Trusted Advisors

The Sectigo Trusted Advisor starts the process by listening to the customer's needs, then proposes the best practices based on the many customers we have successfully deployed. This service includes:

- Trusted Advisors provide comprehensive guidance on how to configure your Branded Certificate Authority hierarchy and delegate administration roles to maximize the usage of trusted identities across departments and partners without the need to centrally manage the addition/deletion/change of digital identities.


Sectigo Cloud Sevice
Root CA (optional)
Optional cross certification to an industry group
Issuing CA Company 1 Organization 1
Issuing CA Company 1 Organization 2
Issuing CA Company 2 Organization 3
Certificate Management
Customer Premises Microsoft CA (optional)
Digital Identities

- Each organization can add/remove their digital identities independently, no need to centralize control
- Self configure delegated administration to suit organizational needs
- All digital identities can be trusted, or the trust can be turned off should circumstances change (i.e. selling an organization or dissolving a partnership
- Full, automated management of discovered of 3rd party certificates

- Trusted Advisors recommend the use cases that best meets your security and productivity needs. It will include integration guidance into existing Enterprise systems.
- Convenient expert, 24x7 support available by phone, email or chat to resolve issues quickly and accurately the first time.

Reliable, Secure Cloud Service

The Sectigo solution is designed to be offered as a Cloud Service. This means that customers are quickly setup to issue digital identities, unlike other vendors that take several weeks. Purchase only what you need, avoiding the costs of setting up the complete infrastructure for the initial pilot. The Sectigo solution is housed in geographically-separated, secure data centers, offering 99.9% high availabil-ity and responsive disaster recovery. Your business is never at risk of down time, costing you money and time.

Due to the nature of PKI technology, authentication, encryption and signing can be done while you are not connected to the Internet or the Sectigo service, unlike competing authentication technologies that require constant cloud service communication. If their server is down or off-line, you can't login.

The Sectigo cloud service holds several certifications that prove our commitment to reliable and secure services. Some of these service include:

- Annual WebTrust audit
- Annual System and Organization Controls 1, 2 and 3

Central Digital Identity Management

The challenges of digital identity management is to ensure that the identity can be 100% automatically installed, renewed for changes to device/user name or security policies, and revoked when the user or device is no longer associated with the Enterprise business. The Sectigo Certificate Manager (CCM) provides a single user interface to manage all the digital identities issued across the entire Enterprise for people, devices and SSL.

The CCM API can be integrated with your Employee HR or device inventory system, so when people/devices leave or join the Enterprise their digital identity can be instantly activated/ deactivated by revocation, without touching the device.

There is no need to replace your Microsoft CA to issue certificates; rather CCM allows you to automate the provisioning of certificates to devices that until now have been manual, such as wireless access points and non-windows Web Servers. The Sectigo certificate authority will replace Microsoft certificates prior to expiry, to applications throughout the Enterprise.

The discovery capability searches your network and active directory looking for certificates that need to be managed. Certificates issued by a third party can be managed, and prior to expiry, automatically updated preventing a service outage.

The CCM supports fully automated certificate life cycle management with a variety of industry standard protocols, with no need to implement costly propriety solutions.

- Simple Certificate Enrollment Protocol (SCEP)
- Windows Client Certificate Enrollment Protocol (MS-WCCE) for desktops and servers.
- Enrollment over Secure Transport (EST) RFC7030
- Automatic Certificate Management Environment (ACME) IETF
- PKCS #12
- Mobile Devices Management.

Contact Sectigo to learn more about Digital Identities for Identity and Access Management.

sales@sectigo.com